Patterns and anti-patterns of embedded development

What security incidents of 2023 teach us (and one of 2024)

Marta Rybczynska - Founder, Syslinbit & Founder, Ygreky

Embedded Linux Conference 2024, Seattle, April 2024

Why?

Who is Marta?


EMBEDDED
OPEN SOURCE
SUMMIT
Community Leadership
MARTA
RYBCZYNSKA
Syslinbit
Critical Software
Supply Chain Security
Embedded Linux
DevOps
SPEAKER
OSS
Vulnerabilities
Emerging Tech
Security
Standards & Specifications

My picks

- Bricked trains
- HTTP/2 protocol implementation issues
- Signing keys leaking
- Linux kernel issues
- The XZ backdoor

Bricked trains

The storyline…
(happened in 2022, published 2023)

- A regional train operator buys trains with **complete maintenance manuals**
- They sign a maintenance contract with someone else than the manufacturer
- What could go wrong?

- Reminder: trains are heavily regulated (safety standards)

The storyline…
(happened in 2022, published 2023)

- Trains do not start after maintenance
- The workshop gets in touch with a reverse engineering group…

- The story made local and international news
- The complete presentation from 37C3: https://youtu.be/XrlrbfGZo2k?si=Frls2AsBvscCzGki

What have they found

- Lock after a long stop
- Lock after a GPS position match
- Date lock
- “Unlock codes”

Image Source:
https://www.youtube.com/watch?v=XrlrbfGZo2k

Anti-patterns

- Nearly every train had a different firmware version
  - Per-device changes?
  - Version control?
  - Automated tests?
- Build paths (in metadata) suggest a local copy, not CI
- Certification - didn’t spot it?
- Developer’s ethics?

HTTP/2 Implementation Issues

HTTP/2 Rapid Reset (CVE-2023-44487)

- Exploited in the wild from August to October 2023
- Issue in implementation of HTTP/2 parallel streams
  - Clients doing massive creation and resetting the request (RST_STREAM frame)
  - Much work on the server side resulting in a Denial of Service
- Most HTTP servers affected

More information with links to products affected : https://nvd.nist.gov/vuln/detail/CVE-2023-44487

Detailed analysis: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/

HTTP/2 Rapid Reset: Patterns and anti-patterns

- A weakness in HTTP/2 protocol definition
  - Streams after RST_STREAM do not count to the stream limit
- Less impact if using careful resource allocation
  - Lighthttpd not affected https://redmine.lighttpd.net/boards/2/topics/11188
    - Processing in batches
    - Stream limit per client at 8
- Usefullness of rate limiting
  - Fix in nghttp2: https://github.com/nghttp2/nghttp2/pull/1961/commits/72b4af6143681f528f1d237b21a9a7aee1738832

Signing keys leaking

MSI signing private keys leak

- Bleeping Computer reported MSI being a target for a ransomware attack
  - See the story: https://www.bleepingcomputer.com/news/security/intel-investigating-leak-of-intel-boot-guard-private-keys-after-msi-breach/
  - A leak of signing private keys for Intel's BootGuard UEFI for MSI products

Key leak: Patterns and anti-patterns

- Secure boot schemas depend on key security
  - Multiple levels of keys
  - Usually a revocation possibility exists
- “Positive point”: seems to have a separate key for each product

Key leak: Patterns and anti-patterns

- Private keys taken by ransomware
  - Likely on a machine in the “main” company network
- No revocation mechanism
  - Attackers may use those keys for years
- Marta’s solution would be (in this case):
    - Two machines not connected to any network, with backup
    - Hardware tokens to store keys

Linux kernel issues

Linux kernel bugs: bpf verifier

- CVE-2023-2163
  - “Incorrect verifier pruning in BPF in Linux Kernel >=5.4 leads to unsafe code paths being incorrectly marked as safe, resulting in arbitrary read/write in kernel memory, lateral privilege escalation, and container escape.”
  - Fix: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=71b547f561247897a0a14f3082730156c0533fed

Linux kernel bugs: nvmet use-after-free

- CVE-2023-5178
  - “A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.”
  - Fix: https://lore.kernel.org/linux-nvme/20231002105428.226515-1-sagi@grimberg.me/
    - Also shows that submission to “stable” is still tricky

Linux kernel bugs

- And dozens others…
- Potential impact
  - External interaction with drivers, control of the system memory…
- Configuration impact
  - Every configuration includes a different set of bugs

Linux kernel bugs: patterns and anti-patterns

- “Do not break the user API” policy
  - Mostly safe update of the kernel version
  - Occassional breakages considered bugs
- CVE assignment
  - High volume (half of CVEs from a typical Yocto Project build)
  - Sometimes hard to find match commit<->CVE
  - This has changed in 2024!

The XZ backdoor

XZ backdoor

- A popular compression library in version 5.6.0 and 5.6.1 included a backdoor
- Included by a co-maintainer
  - Who has been gaining trust from the maintainer for 2 years
- OSS-security discussion: https://www.openwall.com/lists/oss-security/2024/03/29/4

XZ backdoor: Patterns and anti-patterns

- It has been spotted before landing in long term support versions!
- Various build systems and build options are useful
  - Fun fact: the Yocto Project didn't include the update, because it failed to build
  - Embedded has rich set of architectures/compilers/libc…

XZ backdoor: Patterns and anti-patterns

- Sole maintainer of a frequently used project
  - Workload
  - Funding
- Obfuscation, data hiding
  - Payload in binary streams “for tests”
  - M4 scripts, complex regular expressions

Conclusions time

Lessons learnt

- Protocols and standards might contain bugs
- Security best practices are there for a reason
  - If making your life harder - ask a security expert for a fix!
- Development best practices _are_ security measures
  - Mandatory code review
  - Small commits
  - Tests
- Consider your dependencies

Do you want to continue the discussion?

Contact me:

Email: marta.rybczynska@syslinbit.com
LinkedIn: https://www.linkedin.com/in/mrybczynska/